Wide Area Network Security

Effective: January 27, 1997
Revised: March 5, 2004
Owner: David Lee

Purpose

To define the security services available from the Division of Information Technology Services (ITS) for the Wide Area Network (WAN).

Scope

This policy applies to all entities connected to the State WAN backbone ITS for network services. This includes all State agencies, political subdivisions of the State, or quasi-governmental agencies eligible to receive WAN services.

Background

With the recent explosive growth of the Internet and other open networking technologies, an increased risk of security has been recognized. In the past, ITS has built the WAN based on a model for maximum performance and open connectivity. To ensure data integrity, ITS has recognized the need to improve upon the security of the backbone, particularly access to State resources from untrusted networks such as the Internet. ITS believes that there currently are significant security threats to State Government Data Processing resources, the most serious being due to our connection to the Internet.

The implementation of hardware and software to secure sensitive data is an additional cost in terms of time, effort, and funding. ITS is an internal service fund. As such, it is charged with recovering the cost encountered to provide service. The basic WAN rate is based on specific expenses for equipment, services, and overhead. This policy includes detail of security services which *have not been included* in the basic WAN rate calculation. As stated in the policy for basic WAN services, any requirement that exceeds the basic service level will be charged to the requesting agency on an incremental cost basis. Any security services provided by ITS which require custom configuration, additional hardware or software, or other additional cost to implement *may* result in additional charges over and above the basic WAN service rate. This policy defines security which is included in the base connection as well as security services

which may result in additional charges.

Policy

When an agency connects to the State WAN backbone, the following policy applies to security services provided by ITS to ensure data integrity for all WAN customers:

1. The ITS WAN Security Policy will be consistent with and will support the ITS WAN Policy. There will be some overhead incurred in WAN performance for encryption and remote access.

2. The ITS WAN Security policy will be to prioritize apparent security threats and to deal with those considered most serious first.

3. ITS WAN Security will be implemented in an incremental manner with input and assistance from ITS customers. ITS has participated in the formation of the Network Security Implementation and Planning Committee (NSIP), an inter-agency organization which will formulate and establish standards and procedures for network security. ITS will continue to work cooperatively with NSIP to find and implement the best security solutions which may apply to the challenges presented by changing technological and social conditions.

4. ITS will implement packet screening to prevent IP spoofing of ITS-issued addresses from external networks such as the Internet. This service is included as part of the basic WAN service rate provided by ITS.

5. ITS will provide reasonable protection from unauthorized outside penetration of State computing resources for which ITS has custodial responsibility. This includes the mainframe, public access host computers, State Web pages, and other client Web pages where ITS has custodial responsibility. Protection will be provided by implementing firewall technology, packet screening based on destination IP address and source network, encryption of mainframe passwords and login data when connection is established via untrusted external network, and strong authentication of remote users. This effort to protect computing resources may result in additional cost to customers who require remote (Internet) access to State computing resources such as the mainframe.

6. ITS will provide support at the ITS end of Virtual Private Network (VPN) links for secure encrypted customer connectivity to data resources at ITS. Individual agencies and/or customers of the WAN services are responsible for their specific security policy and the implementation of such. VPN and other encryption-related

support will be provided by ITS in accordance with hardware and software standards as approved by the IT PSC. ITS will only support technology which is based upon State standards as approved by the IT PSC. The cost of VPN or encryption capability at the customer side of a trusted link will be incurred by the respective agency. In the case of additional throughput or additional hardware required at the ITS side of the link, some additional cost *may* be charged to the customer to accommodate these needs.

7. ITS will provide a balance between security and performance for the WAN backbone by implementing firewall technology, packet screening, virtual private network links, and strong authentication for remote access to ensure an appropriate level of performance and data integrity.